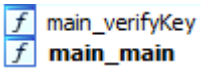
REV - licenseer (Medium)

> Help! I tried writing my new authentication server in go, and I forgot the password!
>
> nc dev.fyrehost.net 54321

Load the downloaded executable file into the IDA. The first thing we do is analyze the functions that the IDA detected. Find the two functions main_main and main_verifyKey.



Let's see what's in the main function of the program. We see that the loop reads user input and passes it to the main_verifyKey function. If the function returns true, then the flag from env is read and output. Let's see what happens in the main_verifyKey function.

```
while ( bufio__ptr_Scanner_Scan((__int64)v7) )
{
  v3 = runtime_slicebytetostring((__int64)v4, v7[4], v7[5], v7[6]);
  if ( main_verifyKey(v3, *((__int64 *)&v3 + 1)) )
  {
    v0 = os_Getenv((__int64)"FLAG", 4LL);
    v1 = runtime_convTstring(v0, v2);
    v6[0] = (__int64)&RTYPE_string;
    v6[1] = v1;
    fmt_Fprintln((__int64)&go_itab__ptr_os_File_comma_io_Writer, os_Stdout, (__int64)v6, 1LL, 1LL);
  }
  else
  {
    v5[0] = (__int64)&RTYPE_string;
    v5[1] = (__int64)&off_4E0C10;
    fmt_Fprintln((__int64)&go_itab__ptr_os_File_comma_io_Writer, os_Stdout, (__int64)v5, 1LL, 1LL);
  }
}
```

In the main_verifyKey function we see that the MD5 hash of the data entered by the user is counted. Then this hash is compared with another hash.

```
*(_QWORD *)&v3 = runtime_stringtoslicebyte((__int64)v10, a1, a2);
*((_QWORD *)&v3 + 1) = crypto_md5_Sum(v3, v5, v6);
*(_OWORD *)v9 = v3;
*(_OWORD *)v11 = 0LL;
v11[0] = runtime_convT2Enoptr((__int64)&RTYPE__16_uint8, (__int64)v9);
v11[1] = v3;
v7 = fmt_Sprintf((__int64)"%x", 2LL, (__int64)v11, 1LL, 1LL);
if ( v8 != 32 )
  return 0;
runtime_memequal(v7, (__int64)"bdc43f04ffda64b1911bcaba87989746");
return v4;
```

Let's try to connect via nc and enter this hash. The program gave out a password - **passWord1234!!**.

Next, we connect to the container of the task, pass the received password and get the flag!

> Flag: **bucket{HASH1NG_IS_S0_FUN_2f47d31e7c28d}**